Northern Kentucky University
**CAREER SERVICES**
UC 225, Highland Heights, KY 41099
careerservices.nku.edu / 859-572-5680

# Phishing Alert: Job Posting Scams

A phishing scam attempts to trick you into providing sensitive personal information (e.g., social security numbers, credit card numbers, and/or banking details) or into sending money or other items of value. These scams come in many forms and disguises, including:

- Employment
- Housing Opportunities
- Online schools and training centers
- Fraudulent eBay sellers
- Emails about being a contest winner or beneficiary of unknown inheritance

## The following characteristics are key red flags:

- You are asked to provide your credit card, bank account numbers, or other personal financial documentation.
- The posting appears to be from a reputable, familiar organization, but the domain in the contact's email address does not match the domain used by representatives of the organization (this is typically easy to determine from the organization's website).
- The position requires an initial investment, such as a payment by wire service or courier.
- The posting includes many spelling and grammatical errors.
- The position initially appears as a traditional job, but upon further research, it sounds more like an independent contractor opportunity.
- You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).
- You unexpectedly receive a large check (checks are typically slightly less than $500).
- You are asked to provide a photo of yourself.
- The position is for any of the following: envelope stuffers, home-based assembly jobs, online surveys.
- The posting neglects to mention specific job responsibilities. Instead, the description focuses on the amount of money to be made.
- The position indicates a first-year compensation that is in high excess to the average compensation for that type of position.
- The salary range listed is very wide (e.g., "employees can earn from $40K - $80K the first year!")
- The employer's phone number, fax number and/or email address does not appear connected to an actual business organization in a Google search.
- The employer contacts you by phone but there is no way to call them back. The number is not available.
- The employer tells you that they do not have an office set-up in your area, and will need you to help them get it up and running.

## How to avoid these scams:

- Review the organization's website. Does it have an index that informs you with details about the organization or does it only contain information about the job you are interested in? Scammers often create quick, basic web pages that seem legitimate at first glance.
- Google the organization's name and the word "scam" (e.g., Organization X Scam), if the results show several scam reports concerning this organization, stay away.
- Watch for anonymity. If it is difficult to find an address, actual contact, organization name, etc., proceed with caution. Fraudulent postings are illegal, so scammers will try to keep well hidden.
- Search the Better Business Bureau (BBB) at https://www.bbb.org/

**If you have concerns about an employer or a posted job, internship, or co-op position, contact Career Services at (859) 572-5680 or careerservices@nku.edu.**

**If you feel you may be a victim of a scam, contact University Police at 859-572-5500 or the Office of Student Conduct, Rights and Advocacy at 859-572-5147 (Student Union 301).**

*(Adapted from handout by CNU's Center for Career Planning, which compiled the information from the LinkedIn NACElink Users Listserv and Symplicity Corporation.)*